

CLAIMS

What is claimed is:

- 1 1. A method comprising:
2 receiving notification of a distributed denial of service attack;
3 establishing security authentication from an upstream router from which attack
4 traffic, transmitted by one or more attack host computers, is received; and
5 once security authentication is established, transmitting one or more filters to
6 the upstream router such that attack traffic is dropped by the upstream router, thereby
7 terminating the distributed denial of service attack.
- 1 2. The method of claim 1, wherein detecting the attack traffic further
2 comprises:
3 monitoring network traffic received by an Internet host; and
4 when a distributed denial of service attack is detected, notifying the Internet
5 host of the distributed denial of service attack.
- 1 3. The method of claim 1, wherein establishing security authentication
2 further comprises:
3 transmitting a security authentication request to the upstream router including
4 authentication information, the authorization information including a destination
5 address of the attack traffic; and
6 receiving authorization for establishment of security authentication from the
7 upstream router.
- 1 4. The method of claim 1, wherein the transmitting the one or more filters
2 further comprises:
3 identifying attack traffic characteristics of the attack traffic received by an
4 Internet host;
5 generating one or more filters based on the identified attack traffic
6 characteristics, such that the one or more filters direct the upstream router to drop
7 network traffic matching the attack traffic characteristics;

8 digitally signing the one or more filters using a digital certificate of the
9 Internet host; and
10 transmitting the one or more digitally signed filters to the upstream router.

1 5. A method comprising:
2 establishing security authentication of an Internet host under a distributed
3 denial of service (DDoS) attack;
4 receiving one or more filters from the Internet host;
5 when security authentication is established, verifying that the one or more
6 filters select only network traffic directed to the Internet host; and
7 once verified, installing the one or more filters such that network traffic
8 matching the one or more filters is prevented from reaching the Internet host.

1 6. The method of claim 5, wherein establishing security authentication
2 further comprises:
3 receiving a request for security authentication including authentication
4 information from the Internet host;
5 selecting the authentication information from the security authentication
6 request; and
7 authenticating an identity of the Internet host based on the selected
8 authentication information.

1 7. The method of claim 5, wherein the receiving the one or more filters
2 further comprises:
3 authenticating a source of the one or more filters received as the Internet host;
4 once authenticated, verifying that a router administrator has set a DDoS
5 squelch time to live value for received filters;
6 once verified, generating a filter expiration time for each filter based on the
7 time to live value, such that the filters are uninstalled once the expiration time expires;
8 verifying that an action component of each of the filters is drop; and
9 otherwise, disregarding the one or more filters received from the Internet host.

1 8. The method of claim 5, wherein verifying the one or more filters
2 further comprises:
3 selecting a destination address component for each of the one or more filters
4 received from the Internet host;
5 comparing the selected destination address components against an address of
6 the Internet host;
7 verifying that the selected destination addresses matches the Internet host
8 address; and
9 otherwise, disregarding the one or more filters received from the Internet host.

1 9. The method of claim 5, wherein installing the one or more filters
2 further comprises:
3 selecting network traffic matching one or more of the filters received from the
4 Internet host; and
5 dropping the selected network traffic such that attack traffic received from one
6 or more attack host computers by the Internet host is eliminated in order to terminate
7 the distributed denial of service attack.

1 10. The method of claim 5, further comprising:
2 determining, by an upstream router receiving the one or more filters from the
3 Internet host, one or more ports from which the attack traffic matching the one or
4 more filters is being received based on a routing table;
5 selecting a port from the one or more determined ports;
6 determining an upstream router connected to the selected port based on a
7 routing table;
8 securely forwarding the one or more filters received from the Internet host to
9 the detected upstream router as a routing protocol update; and
10 repeating the selecting, determining and utilizing for each of the one or more
11 determined ports.

1 11. A method comprising:
2 receiving a routing protocol update from a downstream router;
3 selecting one or more filters from the routing protocol update received from
4 the downstream router;
5 establishing security authentication of the downstream router;
6 once authentication is established, verifying that the one or more filters select
7 only network traffic directed to the downstream router; and
8 once verified, installing the one or more filters such that attack traffic
9 matching the one or more filters is prevented from reaching the downstream router.

1 12. The method of claim 11, wherein establishing security authentication
2 of the downstream router further comprises:
3 selecting authentication information from the routing protocol update received
4 from the downstream router;
5 once selected, authenticating an identity of the downstream router based on the
6 authentication information;
7 authenticating a source of the one or more filters as the downstream router;
8 once authenticated, verifying that a router administrator has set a DDoS
9 squench time to live value for received filters;
10 once verified, generating a filter expiration time for each filter based on the
11 time to live value, such that the filters are uninstalled once the expiration time expires;
12 verifying that an action component of each of the filters is drop; and
13 otherwise, disregarding the one or more filters received from the downstream
14 router.

1 13. The method of claim 11, wherein verifying the one or more filters
2 further comprises:
3 selecting a destination address component for each of the one or more filters;
4 comparing the selected destination address component against an address of
5 the downstream router;

6 verifying that the selected destination address matches the downstream router
7 address; and
8 otherwise, disregarding the one or more filters received from the downstream
9 router.

1 14. The method of claim 11, further comprises:
2 determining, by an upstream router receiving the one or more filters from the
3 downstream router, one or more ports from which attack traffic matching the one or
4 more received filters is being received;
5 selecting a port from the one or more determined ports;
6 determining an upstream router coupled to the selected port based on a routing
7 table;
8 securely forwarding the one or more received filters to the determined
9 upstream router as a routing protocol update; and
10 repeating the selecting, determining, and forwarding for each of the one or
11 more determined ports.

1 15. A computer readable storage medium including program instruction
2 that directed a computer to function in a specific manner when executed by a
3 processor, the program instructions comprising:
4 receiving notification of a distributed denial of service attack;
5 establishing security authentication from an upstream router from which attack
6 traffic, transmitted by one or more attack host computers, is received; and
7 once security authentication is established, transmitting one or more filters to
8 the upstream router such that attack traffic is dropped by the upstream router, thereby
9 terminating the distributed denial of service attack.

1 16. The computer readable storage medium of claim 15, wherein the
2 instruction of detecting the attack traffic further comprises:
3 monitoring network traffic received by an Internet host; and
4 when a distributed denial of service attack is detected, notifying the Internet
5 host of the distributed denial of service attack.

1 17. The computer readable storage medium of claim 15, wherein
2 establishing security authentication further comprises:
3 transmitting a security authentication request to the upstream router including
4 authentication information, the authorization information including a destination
5 address of the attack traffic; and
6 receiving authorization for establishment of security authentication from the
7 upstream router.

1 18. The apparatus of claim 15, wherein transmitting the one or more filters
2 further comprises:
3 identifying attack traffic characteristics of the attack traffic received by an
4 Internet host;
5 generating one or more filters based on the identified attack traffic
6 characteristics, such that the one or more filters direct the upstream router to drop
7 network traffic matching the attack traffic characteristics;
8 digitally signing the one or more filters using a digital certificate of the
9 Internet host; and
10 transmitting the one or more digitally signed filters to the upstream router.

1 19. A computer readable storage medium including program instruction
2 that directed a computer to function in a specific manner when executed by a
3 processor, the program instructions comprising:
4 establishing a security authentication of a downstream device;
5 once security authentication is established, verifying that one or more filters
6 from the downstream device select only network traffic directed to the downstream
7 device; and
8 once verified, installing the one or more filters such that network traffic
9 matching the one or more filters is prevented from reaching the downstream device.

1 20. The apparatus of claim 19, wherein establishing security authentication
2 further comprises:
3 receiving a routing protocol update from the downstream device;
4 selecting authentication information from the received routing protocol
5 update;
6 authenticating an identity of the downstream device based on the selected
7 authentication information;
8 once authenticated, selecting the one or more filters from the received routing
9 protocol; and
10 authenticating integrity of the one or more filters based on a digital signature
11 of the filters.

1 21. The apparatus of claim 19, wherein verifying the one or more filters
2 further comprises:
3 authenticating a source of the one or more filters received as the downstream
4 device;
5 once authenticated, verifying that a router administrator has set a DDoS
6 squelch time to live value for received filters;
7 once verified, generating a filter expiration time for each filter based on the
8 time to live, such that the filters are uninstalled once the expiration time expires;
9 verifying that an action component of each of the filters is drop; and
10 otherwise, disregarding the one or more filters received from the Internet host.

1 22. The apparatus of claim 19, wherein verifying the one or more filters
2 further comprises:
3 selecting a destination address component for each of the one or more filters
4 received from the downstream device;
5 comparing the destination address components against an address of the
6 downstream device;

7 verifying that the selected destination addresses matches the downstream
8 device address; and
9 otherwise, disregarding the one or more filters received from the downstream
10 device.

1 23. The computer readable storage medium of claim 19, wherein
2 establishing security authentication further comprises:
3 receiving a request for security authentication including authentication
4 information from the downstream device;
5 selecting the authentication information from the security authentication
6 request; and
7 authenticating an identity of the downstream device based on the selected
8 authentication information.

1 24. The apparatus of claim 19, wherein installing the one or more filters
2 further comprises:
3 selecting network traffic matching one or more of the filters received from the
4 downstream device; and
5 dropping the selected network traffic such that attack traffic received from one
6 or more attack host computers by the downstream device is eliminated in order to
7 terminate a distributed denial of service attack.

1 25. The apparatus of claim 19, further comprising:
2 determining, by an upstream router receiving the one or more filters from the
3 downstream router, one or more ports from which attack traffic matching the one or
4 more received filters is being received;
5 selecting a port from the one or more determined ports;
6 determining an upstream router coupled to the selected port based on a routing
7 table;

8 securely forwarding the one or more received filters to the determined
9 upstream router as a routing protocol update; and
10 repeating the selecting, determining, and forwarding for each of the one or
11 more determined parts.

1 26. An apparatus, comprising:
2 a processor having circuitry to execute instructions;
3 a control plane interface coupled to the processor, the control plane interface
4 to packet processing filters, and to authenticate a source of the packet processing
5 filters; and
6 a storage device coupled to the processor, having sequences of instructions
7 stored therein, which when executed by the processor cause the processor to:
8 establish a security authentication of a downstream device.
9 once security authentication is established, verify that one or more
10 filters from the downstream device select only network traffic directed to the
11 downstream device and
12 once verified, install the one or more filters such that network traffic
13 matching the one or more filters is prevented from reaching the downstream device..

1 27. The apparatus of claim 26, wherein the instruction to establish security
2 authentication further causes the processor to:
3 receive a routing protocol update from the downstream device;
4 select authentication information the received from routing protocol update;
5 authenticate an identity of the downstream device based on the selected
6 authentication information;
7 once authenticated, select the one or more filters from the received routing
8 protocol; and
9 authenticate integrity of the one or more filters based on a digital signature of
10 the filters.

1 28. The apparatus of claim 26, wherein the instruction to receive the one or
2 more filters further causes the processor to:
3 authenticate a source of the one or more filters received as the downstream
4 device;
5 once authenticated, verify that a router administrator has set a DDoS squelch
6 time to live value for received filters;
7 once verified, generate a filter expiration time for each filter based on the time
8 to live, such that the filters are uninstalled once the expiration time expires;
9 verify that an action component of each of the filters is drop; and
10 otherwise, disregard the one or more filters received from the Internet host.

1 29. The apparatus of claim 26, wherein the instruction to verify the one or
2 more filters further causes the processor to:
3 select a destination address component for each of the one or more filters
4 received from the downstream device,
5 compare the destination address components against an address of the
6 downstream device,
7 verify the selected destination addresses matches the Internet host address, and
8 otherwise, disregard the one or more filters received from the downstream
9 device

1 30. The apparatus of claim 26, wherein instruction to install the one or
2 more filters further causes the processor to:
3 select network traffic matching one or more of the filters received from the
4 downstream device, and
5 drop the selected network traffic such that attack traffic received from one or
6 more host attack computers by the downstream device is eliminated in order to
7 terminate a distributed denial of service attack.

1 31. The apparatus of claim 26, wherein the processor is further caused to:
2 determine, by a router receiving the one or more filters from the downstream
3 device, one or more ports from which the attack traffic matching the one or more
4 filters is being received based on a routing table,
5 determine one or more upstream routers connected to the determined ports,
6 establish a secure connection with each of the one or more upstream routers,
7 and
8 forward the one or more filters received from the downstream device to the
9 one or more upstream routers.

1 32. The apparatus of claim 26, wherein the instruction to establish security
2 authentication further causes the processor to:
3 receiving a request for security authentication including authentication
4 information from the downstream device;
5 decrypting the received authentication information;
6 selecting the authentication information from the security authentication
7 request; and
8 authenticating an identity of the downstream device based on the selected
9 authentication information.

1 33. A system comprising:
2 an Internet host;
3 a wide area network; and
4 a router coupled between the Internet host and the wide area network, the
5 router having:
6 a processor having circuitry to execute instructions;
7 a control plane interface coupled to the processor, the control plane interface
8 to receive packet processing filters, and to authenticate a source of the packet
9 processing filters; and
10 a storage device coupled to the processor, having sequences of instructions
11 stored therein, which when executed by the processor cause the processor to:

12 establish security authentication of an Internet host under a distributed
13 denial of service (DDoS) attack;
14 receive one or more filters from the Internet host;
15 when security authentication is established, verify that the one or more
16 filters select only network traffic directed to the Internet host; and
17 once verified, install the one or more filters such that network traffic
18 matching the one or more filters is prevented from reaching the Internet host.

1 34. The system of claim 33,
2 wherein the Internet host receives notification of a distributed denial of service
3 attack, establishes security authentication from an upstream router from which the
4 attack traffic, transmitted by one or more attack host computers, is received, and
5 transmits one or more filters to the upstream router such that attack traffic is dropped
6 by the upstream router, thereby terminating the distributed denial of service attack.

1 35. The system of claim 33, wherein the processor is further caused to:
2 determine, by a router receiving the one or more filters from a downstream
3 device, one or more ports from which the attack traffic matching the one or more
4 filters is being received based on a routing table,
5 determine one or more upstream routers connected to the determined ports,
6 and
7 securely forward the one or more filters received from the downstream device
8 to the one or more upstream routers as a routing protocol update.